REMARKS

Claims 1, 3-16 and 18 were pending at the time of the Office Action. In this Amendment, claims 1, 7, 10 and 12 have been amended to clarify an aspect of the invention. Support is found in, for example, paragraphs [0049], [0068]-[0071], and [0083]-[0084] of the application-as-published. Claims 1, 3-16 and 18 are currently pending for examination, of which claims 1, 7, 10 and 12 are independent. Care has been exercised not to introduce new matter.

REJECTION OF CLAIMS UNDER 35 U.S.C. § 103

Claims 1, 3, 5, 7, 8, 10-16 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohta et al. (U.S. Patent No. 7,158,637, hereinafter "Ohta"), in view of Ehrsam et al. (U.S. Patent No. 4,238,854, hereinafter "Ehrsam"). Claims 6 and 9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ohta in view of Ehrsam applied above, and further in view of Porter et al. (U.S. Patent Application Publication No. 2003/0226029, hereinafter "Porter"). The rejections are respectfully traversed for the following reasons.

Independent claims 1 and 7, in pertinent part, recites "the cryptographic processing unit that receives a plurality of respectively belonging to two or more different cryptographic input and output processes via the bus and in a time-division manner, refers to identifying information attached to the command, identifies to which cryptographic input and output process the received command belongs, and rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input and output process to which the command belongs." As disclosed in FIGS. 1 and 8, illustrating one example of what is recited in claim 1, to manage the sequence of commands executed for each process system, a sequence ID for identifying a process system is assigned to the command for each process

system, thereby allowing the sequence ID to identify to which process system the received command belongs. Cryptographic input/output processing for writing license data is divided into secure commands such as the certificate output command (S102), the challenge key input command (S120), the session key preparation command (S132), the session key output command (S142), the license data input command (S158), and the license data write command (S168), thereby assigning the sequence ID to a series of cryptographic input/output processing. This makes it possible to identify to which process system a secure command belongs even when a plurality of cryptographic input/output processing are executed simultaneously. This allows for properly managing the sequence of the secure commands and securely managing keys or data exchanged using the secure commands for each process system. (See paragraphs [0049], [0068]-[0071], and [0083]-[0084] of the application-as-published)

The proposed combination of Ohta, Ehrsam and Porter fails to disclose the limitations of claims 1 and 7 regarding "the cryptographic processing unit that receives a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus and in a time-division manner, refers to identifying information attached to the command, identifies to which cryptographic input and output process the received command belongs, and rejects the execution of the command when having detected that the command is an incorrectly sequenced command in the cryptographic input and output process to which the command belongs."

Ohta's authentication processing unit 104 performs authentication processing in parallel to the encryption processing or the decryption processing of the encryption processing unit 102. Ohta's authentication processing and decryption/encryption processing are not subdivided to plural subprocesses in a time-division manner. So, commands are not assigned to subprocesses

of the authentication processing and decryption/encryption processing. In contrast, claim 1 requires "the cryptographic processing unit" to "receives a plurality of subprocesses respectively belonging to two or more different cryptographic input and output processes via the bus and in a time-division manner," and to "identify[ies]y to which cryptographic input and output process the received command belongs."

Ehrsam, which was cited for managing the sequence of commands, and Porter, which was cited for the storage device, fail to cure deficiencies of Ohta, as well.

In addition, the proposed combination of Ohta, Ehrsam and Porter fails to disclose the limitations of claims 1 and 7 regarding "a bus for receiving the command from the host device, the bus being deallocated for another command when the command is issued."

Accordingly, as each and every limitation must be disclosed or suggested by the cited prior art references in order to establish a *prima facie* case of obviousness (*see*, M.P.E.P. § 2143.03) and for at least the foregoing reasons the proposed combination of Ohta, Ehrsam and Porter fails to do so, it is respectfully submitted that claims 1 and 7 and claims dependent thereupon are patentable over the combination of Ohta, Ehrsam and Porter.

Independent claims 10 and 12 recites similar limitations to claim 1 regarding "when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input and output processes the command belongs and to manage the sequence of commands executed in each cryptographic input and output process, and the controller that issues the command via the bus electrically connecting the host device and the storage device and deallocates the bus for another command," and "allowing the host device to deallocate the bus for another command, and identifying information is attached to the command to identify to which one of the plurality of cryptographic input and

output processes, being performed simultaneously by the storage device, the command belongs," respectively. Therefore, claims 10 and 12 and claims dependent thereupon are patentable over the cited prior art for the same reasons as claims 1 and 7.

Conclusion

In view of the above amendments and remarks, Applicants submit that this application should be allowed and the case passed to issue. If there are any questions regarding this Amendment or the application in general, a telephone call to the undersigned would be appreciated to expedite the prosecution of the application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Hosang Lee
Registration No. L00,295

Please recognize our Customer No. 20277 as our correspondence address.

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 SAB/HL
Facsimile: 202.756.8087
Date: April 28, 2009